Claims

1. An electronic security device comprising means for receiving and outputting signals when in an authorised use state, a real time clock for determining whether a predetermined real time period has expired and, if so, seeking an authorisation, means for verifying the authorisation, and means for configuring the device into an unauthorised use state in the event that a correct authorisation is not received in time.

2. An electronic device according to claim 1, in which the device is adapted to receive encrypted authorisation codes.

3. An electronic device according to claim 1 or claim 2, in which when in an unauthorised use state the device received input signals, encrypts them and outputs the encrypted signals.

4. An electronic device according to claim 1 or claim 2, in which the device comprises means whereby when in an unauthorised use state, the device reduces the frequency at which inputs are transmitted to an input receiver.

5. An electronic device according to any preceding claim, in which the device includes means for generating a random (which expression includes pseudo-random) number and means for encrypting the random number.

6. An electronic device according to claim 5, in which the device includes means for performing a predetermined mathematical operation on the random number.

7. An electronic device according to claim 5 or claim 6, in which the device includes means for encrypting and decrypting data.

8. An electronic device according to claim 7, in which the encryption is according to a public key algorithm.

9. An electronic device according to any preceding claim, in which the device additionally comprises a means for periodically checking the real time clock against a predetermined time period.

10. An electronic device according to claim 9, in which the periodic checking means comprises a counter which upon reaching a predetermined number initiates the check and means for re-setting the counter.

11. An electronic device according to any preceding claim, in which the device comprises a dedicated power supply.

12. An electronic device according to claim 11, in which the device is embodied in a plug-in module, which plug in module suitably comprises a power source such as a battery.

13. An electronic apparatus comprising a security device according to any one of claims 1 to 12.

14.An electronic apparatus according to claim 13, in which the security device is located between an electronic output device and an electronic input device.

15. An electronic apparatus according to claim 14, in which when in an unauthorised use state the device reduces the frequency at which key presses are transmitted to or within the electronic apparatus.

16. A digital electronic computer comprising a security device according to any one of claims 1 to 12.

17. A method of operating an electronic device comprising a security device which receives output signals when in an authorised use state, the method comprising the steps of using a real time clock to determine whether a predetermined real time period has expired and, if so, seeking an authorisation, checking whether the authorisation is acceptable and configuring the device in an unauthorised use state in the event that a correct authorisation is not received in time.

18. A method according to claim 17, in which the authorisation code is encrypted.

19. A method according to claim 17 or claim 18, in which when in an unauthorised use state the device receives input signals, encrypts them and outputs the encrypted signals.

20. A method according to claim 17 or claim 18, in which when in an unauthorised use state, the device reduces the frequency at which inputs are transmitted to an input receiver.

21. A method according to any one of claims 17 to 20, in which the device generates a random (which expression

includes pseudo-random) number and encrypts the random number.

22. A method according to claim 21, in which the device performs a predetermined mathematical operation on the random number.

23. A method according to claim 21 or claim 22, in which the device encrypts and decrypts data.

24. A method according to claim 23, in which the encryption is according to a public key algorithm.

25. A method according to claim 23 or claim 24, in which the encrypted number is transmitted to a verification station which verification station decrypts the encrypted number and verifies it against a number previously supplied to the electronic device.

25. An electronic system adapted and configured to operate according to any one of claims 17 to 25.